

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY**

UNITED STATES OF AMERICA	:	Hon. Katharine S. Hayden
v.	:	Criminal No. 10-114
KENNETH LOWSON, a/k/a "Money,"	:	
KRISTOFER KIRSCH, a/k/a "Robert Woods,"	:	
JOEL STEVENSON, and	:	
FAISAL NAHDI	:	

**UNITED STATES' OPPOSITION TO DEFENDANTS' MOTION
TO DISMISS THE SUPERCEDING INDICTMENT**

PAUL J. FISHMAN
United States Attorney
970 Broad Street
Newark, New Jersey 07102
(973) 645-2700

On the Memorandum:

EREZ LIEBERMANN
SETH B. KOSTO
Assistant United States Attorneys
District of New Jersey

JOSH GOLDFOOT
Trial Attorney
Computer Crime and Intellectual Property Section
U.S. Department of Justice

TABLE OF CONTENTS

INTRODUCTION	1
STATEMENT OF FACTS	3
LEGAL STANDARD	8
I. DEFENDANTS TOOK TRADITIONALLY RECOGNIZED PROPERTY RIGHTS FROM ONLINE TICKET VENDORS	9
II. DEFENDANTS CIRCUMVENTED CODE-BASED AND CONTRACT-BASED RESTRICTIONS ON ACCESS IN VIOLATION OF SECTION 1030	18
III. THE CHARGES IN THE SUPERCEDING INDICTMENT ARE NOT VAGUE, AND THE RULE OF LENITY IS INAPPLICABLE	25
IV. COUNTS 11 THROUGH 20 OF THE SUPERCEDING INDICTMENT DISTINCTLY ALLEGE UNAUTHORIZED ACCESS AND FRAUD	28
V. DEFENDANTS OBTAINED “INFORMATION” UNDER SECTION 1030(a)(2)(C)	30
VI. DEFENDANTS DAMAGED ONLINE TICKET VENDORS’ COMPUTERS BY IMPAIRING THE AVAILABILITY OF DATA WITHOUT AUTHORIZATION	32
CONCLUSION	34

TABLE OF AUTHORITIES

Cases

<i>America Online Inc. v. LCGM, Inc.</i> , 46 F. Supp. 2d 444, 450 (E.D. Va 1998)	22, 32
<i>America Online v. National Health Care Disc., Inc.</i> , 121 F. Supp. 2d. 1255 (N.D. Iowa 2000) ...	32, 34
<i>Brett Senior & Assocs. v. Fitzgerald</i> , 2007 WL 2043377 (E.D.P.A. July 13, 2007)	23, 24, 29
<i>Carpenter v. United States</i> , 484 U.S. 19, 26, 27 (1987)	10, 11
<i>Cleveland v. United States</i> , 531 U.S. 12 (2000)	10, 12
<i>Creative Computing v. Getloaded.com LLC</i> , 386 F.3d 930, 936 (9th Cir. 2004)	20
<i>eBay, Inc. v. Digital Point Solutions, Inc.</i> 608 F. Supp. 2d 1156, 1164 (N.D. Cal. 2009)	22
<i>EF Cultural Travel BV v. Zefer Corp.</i> , 318 F.3d 58, 62 (1 st Cir. 2003)	23
<i>Facebook v. Power Ventures, Inc.</i> , No. C. 08-05780 JW (N.D. Cal. Jul. 20, 2010)	19-21, 28
<i>Ford v. Torres</i> , 2009 WL 537563, *9 (E.D. Va. Mar. 3, 2009)	34
<i>Hamling v. United States</i> , 418 U.S. 87, 117 (1974)	9
<i>Hartford Underwriters Ins. Co. v. Union Planters Bank, N.A.</i> , 530 U.S. 1 (2000)	30
<i>Healthcare Advocates v. Harding, Earley, Follmer & Frailey</i> , 497 F. Supp. 2d 627 (E.D.P.A. 2007) .	31
<i>Int'l Airport Centers v. Citrin</i> , 440 F.3d 418 (7 th Cir. 2006)	24
<i>Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda</i> , 390 F. Supp. 2d 479 (D. Md. 2005)	23, 24
<i>Leocal v. Ashcroft</i> , 543 U.S. 1, 11 n.8 (2004)	23
<i>LVRC Holdings v. Brekka</i> , 581 F.3d 1127, 1134 (9 th Cir. 2009)	23, 24
<i>Moulton v. VC3</i> , 2000 WL 33310901, *6 (N.D. Ga. Nov. 7, 2000)	34
<i>Register, Inc. v. Verio, Inc.</i> , 126 F. Supp. 2d 238, 251 (S.D.N.Y. 2000)	22
<i>Ticketmaster LLC v. RMG Technologies</i> , 507 F. Supp. 2d 1096, 1112 (C.D. Cal. 2007)	19
<i>United States v. Al Hedaithy</i> , 392 F.3d 580, 590 (3d Cir. 2006)	9, 10, 12-15, 17

<i>United States v. Alkaabi</i> , 223 F. Supp. 2d 583, 585 (D.N.J. 2002)	14
<i>United States v. Alsugair</i> , 256 F. Supp.2d 306, 315 (D.N.J. 2003)	14, 15, 17
<i>United States v. Besmajian</i> , 910 F.2d 1153, 1154 (3d Cir. 1990)	9
<i>United States v. Bruchhausen</i> , 977 F.2d 464 (9 th Cir. 1992)	15-17
<i>United States v. Carlson</i> , 209 Fed. Appx. 181, 2006 WL 3770611 (3d Cir. 2006)	33
<i>United States v. DiFronzo</i> , 26 F.3d 133 (9th Cir. 1994)	16
<i>United States v. Drew</i> , 259 F.R.D. 449 (N.D. Cal. 2009)	25-28, 31
<i>United States v. Fullmer</i> , 584 F.3d 132, 152 (3d Cir. 2009)	25, 26, 28
<i>United States v. Gray</i> , 405 F.3d 227, 234 (4th Cir. 2007)	10
<i>United States v. Harper</i> , 32 F.3d 1387 (9th Cir. 1994)	16
<i>United States v. Henry</i> , 29 F.3d 112, 115 (3d Cir. 1994)	9, 15
<i>United States v. John</i> , 597 F.3d 263, 271 (5 th Cir. 2010)	22, 24
<i>United States v. Kemp</i> , 500 F.3d 257, 280 (3d Cir. 2007)	9
<i>United States v. Mazurie</i> , 419 U.S. 544, 550 (1975)	25
<i>United States v. Nosal</i> , 2010 WL 934257, *6 (N.D. Cal. Jan. 6, 2010)	23, 24
<i>United States v. Panarella</i> , 277 F.3d 678, 694, 690 n.7 (3d Cir. 2002)	9, 20
<i>United States v. Salman</i> , 378 F.3d 1266, 1267 (11th Cir.2004)	23
<i>United States v. Salum</i> , 257 Fed. Appx. 225, 230 (11th Cir. 2007)	22, 24
<i>United States v. Schuster</i> , 467 F.3d 614, 616 (7th Cir. 2006)	34
<i>United States v. Schwartz</i> , 924 F.2d 410, 421 (2d Cir.1991)	10, 13, 14, 16, 17
<i>United States v. Weinstein</i> , 762 F.2d 1522, 1533 (11th Cir. 1985)	17

Statutes

18 U.S.C. § 1030	2, 18, 20, 22-24, 27, 29-32
18 U.S.C. § 1030(a)(4)	29
18 U.S.C. § 1030(a)(5)	32
18 U.S.C. § 1030(e)(8)	33

Rules

Fed. R. Crim. P. 7(c)(1)	8
--------------------------------	---

Other Authorities

http://en.wikipedia.org/wikipedia/encryption (visited Jul. 21, 2010)	4
http://www.zdnet.com/news/ticketmaster-sues-ebays-stubhub-over-sales-tactics/151906 (visited Jul. 26, 2010)	12
Orin S. Kerr, <i>Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes</i> , 78 N.Y.U. L. Rev. 1596, 1650-51 (2003)	20
S. Rep. 104-357, 104th Congress, 2nd Session, 1996 WL 492169 at 8 (1996)	27, 31
S. Rep. 99-432 at 8-9 (1986)	29, 31

INTRODUCTION

Defendants lied about who they were. They lied about their business model. They lied when they impersonated thousands of individual ticket buyers. And they lied when they established thousands of false e-mail addresses and domain names.

Defendants lied because they wanted Wiseguy Tickets to become the premier distributor of 1.5 million prime tickets to concerts and sporting events. The right to sell those tickets to the public was worth millions, but online ticket vendors, artists, promoters, and venues — the holders of those rights — would not knowingly sell to defendants. So instead of negotiating for their own distribution rights or otherwise acquiring the tickets legitimately, defendants got the tickets through fraud and deception.

When defendants received cease and desist letters and notice that their access to online ticket vendors' websites was unwelcome, they ignored these demands or lied in response. When the victims blocked defendants' computers from their websites, defendants simply attacked from different computers. And when the victims set up other technical barriers against defendants' ticket-buying software, defendants hired computer programmers to try every method they could to beat those security measures.

Defendants do not deny that they lied or took things that the victims did not want to sell to them. Instead, defendants argue that the wire fraud statute does not protect what they took. In moving to dismiss the wire fraud allegations, defendants attempt to revisit the question of whether valuable property rights such as exclusivity, the right to choose the market for one's goods, and good will are "property" within the meaning of the wire fraud statute, ignoring controlling Third Circuit precedent in the process. As that precedent shows, the wire fraud statute protects against the taking of the rights alleged in the Superceding Indictment.

In challenging the Computer Fraud and Abuse Act (“Section 1030”) counts, defendants do not ignore precedent; instead, they ignore the allegations in the Superceding Indictment. Defendants base their entire argument on “*the Government’s theory that alleged breaches of terms of use constitute unauthorized access....*” Def.’s Br. at 8. In a brief that barely mentions the Superceding Indictment yet purports to aid the Court, *amici* similarly criticize “the Government’s argument” that “users violate federal law every time they breach the terms of service unilaterally imposed by websites, regardless of how unreasonable those terms may be.” Am. Br. at 20.

This is not the Government’s theory.

Defendants’ access was not illegal only because defendants intentionally violated terms of service. It was illegal because defendants hacked the victims’ computers by defeating barriers to access — software code that online ticket vendors used to protect their websites. These restrictions included code that denied access to the victims’ networks to IP addresses that appeared to be operating automated programs, code intended to block automated programs, and other technological blocks.

Defendants claim they merely violated vague terms of service. Words, they say, cannot define criminally unauthorized access. But defendants did not hire Bulgarian computer programmers to get around nouns and verbs. Defendants hired computer programmers to attack computer code that was blocking their access to the online ticket vendors’ websites.

This is not the case for academic debate about whether terms of service alone can define authorized access under Section 1030. This is a case about fraud and about access restrictions — technical and otherwise — that defendants willfully attacked and circumvented. The Superceding Indictment plainly states valid offenses and, thus, cannot be dismissed.

STATEMENT OF FACTS

Defendants Kenneth Lowson, Kristofer Kirsch, and Joel Stevenson owned and directed the various companies operating as Wiseguy Tickets (“Wiseguys”), a business engaged in acquiring tickets to concerts, live theater, and sporting events (“Events”) from vendors on the primary market and selling those tickets on the secondary market. (Defendant Faisal Nahdi, who has fled the United States and refused to return, is not before the Court.) The Superceding Indictment charges defendants with one count of conspiracy to commit wire fraud and computer intrusion and 42 related substantive counts.

Online Distribution of Tickets

During the period charged in the Superceding Indictment, venues, promoters, artists, and sports teams (“Venue Entities”) distributed tickets online. Superceding Indictment, ¶ 2(a). Venue Entities held the exclusive right to determine who would distribute their tickets. Once they selected a distribution outlet, such as Ticketmaster, Telecharge, Tickets.com, Musictoday, or LiveNation (“Online Ticket Vendors”), Venue Entities negotiated exclusive agreements with Online Ticket Vendors (“Event Agreements”). *Id.*, ¶ 2(b). To Online Ticket Vendors, exclusive distribution rights and the right to define to whom they sold were valuable property interests that were a critical part of the negotiated Event Agreements. *Id.*, ¶ 2(c). Exclusive distribution rights increased Online Ticket Vendors’ revenue and also generated goodwill for them. *Id.*

As part of Event Agreements, Venue Entities and Online Ticket Vendors set terms of sale, including Event ticket prices and the maximum amount of tickets one person could purchase per show. *Id.*, ¶¶ 2(h) & 2(j). Often, Venue Entities and Online Ticket Vendors did not set prices at the highest price the market would tolerate, *i.e.*, not at fair market value. Instead, other factors led Venue Entities and Online Ticket Vendors to set artificially low ticket prices,

including the goal of allowing fans to afford the tickets. *Id.*, ¶ 2(e). For popular events, low ticket prices contributed to very high demand, with tickets selling out in a matter of minutes. *Id.*, ¶¶ 2(I) & 2(j). Despite this high demand, both the Venue Entities and Online Ticket Vendors sought to ensure fair access to the tickets on a first-come, first-served basis and thus established virtual queues for the tickets. *Id.*, ¶ (2)(I).

Restricting Access to the Buypage

To keep the virtual queue fair, Online Ticket Vendors controlled access to the “portions of their websites that could actually be used to purchase Event tickets” (“Buypages”). *Id.*, ¶ 2(j). Computer programs that purchased tickets automatically were not authorized to access Buypages. *Id.*, ¶ 2(k). Online Ticket Vendors enforced these access restrictions through computer code that protected their websites and through terms of service, cease and desist demands, and litigation.

The computer code-based restrictions on access consisted of the following (“Code-Based Restrictions”):

- *Encryption.* Online Ticket Vendors restricted access to Buypages through encryption (“Buypage Encryption”). *Id.*, ¶ 9(c).¹ Buypage Encryption was intended to ensure that any user accessing Online Ticket Vendors’ websites had to follow a particular set of steps before accessing Buypages. That set of steps contained additional restrictions, explained below.
- *CAPTCHA* (“Completely Automated Public Turing test to tell Computers and Humans Apart”). Website owners used CAPTCHA to restrict access to their websites. To visit Buypages and purchase tickets, users had to answer

¹ “Encryption is the process of transforming information using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.” <http://en.wikipedia.org/wikipedia/encryption> (visited Jul. 21, 2010).

CAPTCHA challenges, questions designed to be answerable only by human computer users, not by automated programs. *Id.*, ¶ 2(l). If a user did not complete a CAPTCHA challenge correctly, the user could not access a Buypage.

CAPTCHA challenges are not unique to ticket websites. Instead, these security measures restrict access on many e-commerce websites, including Facebook, Google, and Yahoo!, which permit access to human users but restrict access to automated programs.

- *Audio CAPTCHA*. A version of CAPTCHA that offered the visually impaired an opportunity to respond to CAPTCHA challenges by listening to sounds distinguishable only to the human ear and was therefore designed to block access to automated programs. *Id.*, ¶ 2(o).
- *Proof of Work*. Computer code intended to restrict access to automated programs by forcing automated programs to slow down to the point that it was not worth using them to purchase tickets. *Id.*, ¶ 2(q).
- *Internet Protocol Blocks (“IP Blocks”)*. Online Ticket Vendors electronically blocked access to Buypages and — in some cases — to their entire websites to any computer using an IP address associated with automated ticket purchasing. Through IP Blocks, Ticketmaster restricted complete access to its websites from thousands of IP addresses used by Wiseguys. *Id.*, ¶ 2(s).

In addition to Code-Based Restrictions, the Online Ticket Vendors restricted access to Buypages using other restrictions (“Contract-Based Restrictions”):

- *Cease and Desist Demands*. Online Ticket Vendors identified automated programs attempting to access their systems and made telephone calls and sent

cease and desist demands to inform automated purchasers that their access was unauthorized. *Id.*, ¶ 2(r). On or about June 5, 2005, for example, an Internet Service Provider received a cease and desist letter regarding computers that Wiseguys had leased (under false names). The letter, which defendant Kirsch forwarded to defendant Lawson, demanded that Wiseguys “immediately cease and desist any and all connection to ticketmaster.com.” *Id.*, ¶ 46(f). On or about August 10, 2005, Ticketmaster’s legal counsel wrote to defendant Lawson demanding that Wiseguys cease its conduct. *Id.*, ¶ 2(r). In 2008, Ticketmaster also contacted companies hosting Wiseguys’ computers and demanded that the companies and their clients not use automated programs to access Ticketmaster’s websites. *Id.*

- *Terms of Service.* Online Ticket Vendors used both multi-paragraph and more concise terms of service expressly restricting the use of automated programs. Ticketmaster, for example, had the following term listed under its CAPTCHA challenges: “You do not have permission to access this website if you are using an automated program.” *Id.*, ¶ 2(n) (emphasis supplied).
- *Legal Action.* Online Ticket Vendors also brought lawsuits to enforce their restrictions on access. *Id.*, ¶ 40.

Defendants Knew Online Ticket Vendors Would Not Sell to Them

Defendants knew that Online Ticket Venders would not sell them tickets if they were truthful about their identities. Defendants used shell companies to hide their activities, *Id.*, ¶ 46, and planned and deployed “stealth measures” to avoid getting caught. *Id.*, ¶¶ 36 & 47(e). Defendants changed corporate names and used strawman transactions involving Wiseguy

Tickets, Smaug, Inc., and Seats of San Francisco to avoid detection. *Id.*, ¶¶ 1(c), 1(g), & 46(a). They also used different corporate names to register for computer servers and lied to the companies hosting their equipment about their true identities and how they used their computers. *Id.*, ¶ 37 (defendant Kirsch stating that his company provided “hotel brokering services”) & ¶ 46(c) (defendant Kirsch identifying himself as “Robert Woods”). Instead of purchasing tickets as “Wiseguy Tickets,” defendants used names and credit cards belonging to thousands of others to disguise Wiseguys’ automated efforts to buy tickets. *Id.*, ¶¶ 20-21.

Defendants Knew Their Access Was Restricted

Defendants knew they were not authorized to access Online Ticket Vendors’ websites. For example, defendants wrote software designed to check a box on Ticketmaster’s website indicating their acceptance of its terms of service — one of the restrictions that Ticketmaster placed between customers and Buypages. *Id.*, ¶ 26. Defendants also received and discussed cease and desist demands. *Id.*, ¶¶ 46(e) & (f). Moreover, defendants had actual knowledge of Online Ticket Vendors’ Code-Based Restrictions and constantly discussed ways to circumvent those restrictions. *Id.*, ¶ 47(c) (defendants discussing the fact that “[Ticketmaster] can just block all of [the IP addresses] in a single sweep.”). To get around IP Blocks, defendants sought to employ a computer network of 100,000 IP addresses. *Id.*, ¶ 47(e).

Defendants Actively Circumvented Restrictions on Access

The Superceding Indictment alleges that defendants tried to defeat Online Ticket Vendors’ security measures. *Id.*, ¶ 5. To do this, defendants hired sophisticated computer programmers from Bulgaria, among other countries, to get automated access to Buypages despite the Code-Based Restrictions. *Id.*, ¶¶ 1(I) & 7. This included trying to beat Buypage Encryption. *Id.*, ¶ 9(c). It also included using Optical Character Recognition (“OCR”) and other computer

code to beat CAPTCHA, *id.*, ¶ 9(a); writing programs to circumvent the Proof of Work restrictions, *id.*, ¶ 10(a); and deploying a network of 100,000 IP addresses to avoid IP Blocks, *id.*, ¶¶ 15 & 47(e).

Defendants' attempts to gain unauthorized access through automation succeeded. They thereby became the *de facto* distributors of more than 1.5 million tickets that Venue Entities and Online Ticket Vendors would not willingly have sold directly to them. Defendants made approximately \$28,000,000 in profits. *Id.*, ¶¶ 52-55.

Defendants' Scheme to Take Customers from Online Ticket Vendors

By 2008, defendants had been so successful at beating Online Ticket Vendors' Code-Based Restrictions that defendant Lowson established Renaissance Events Management ("REM"), a company that would compete with Ticketmaster for the right to distribute Event tickets on behalf of artists, promoters, and venues. *Id.*, ¶ 41. Defendant Lowson held REM out to be a company that could — unlike Online Ticket Vendors — keep tickets out of the hands of brokers using automated systems. Defendants thus offered themselves as a solution to the very problem that they created.

LEGAL STANDARD

Under Fed. R. Crim. P. 7(c)(1), an indictment must contain only a "plain, concise and definite written statement of the essential facts constituting the offense charged." An indictment is sufficient so long as it:

(1) contains the elements of the offense intended to be charged, (2) sufficiently apprises the defendant of what he must be prepared to meet, and (3) allows the defendant to show with accuracy to what extent he may plead a former acquittal or conviction in the event of a subsequent prosecution. Moreover, no greater specificity than the statutory language is required so long as there is sufficient factual orientation to permit the defendant to prepare his defense and to invoke double jeopardy in the event of a subsequent prosecution.

United States v. Kemp, 500 F.3d 257, 280 (3d Cir. 2007) (internal citations omitted); *Hamling v. United States*, 418 U.S. 87, 117 (1974) (similar standard under Constitutional notice requirements).

On a motion to dismiss, the Court must consider the entire indictment. *United States v. Panarella*, 277 F.3d 678, 694, 690 n.7 (3d Cir. 2002). “In considering a defense motion to dismiss an indictment, the district court accepts as true the factual allegations set forth in the indictment.” *United States v. Besmajian*, 910 F.2d 1153, 1154 (3d Cir. 1990). “[F]or purposes of Rule 12(b)(2), a charging document fails to state an offense if the specific facts alleged in the charging document fall beyond the scope of the relevant criminal statute, as a matter of statutory interpretation.” *Panarella*, 277 F.3d at 685.

This black letter rule is especially important in this case, because defendants and *amici* improperly ignore the vast majority of the allegations in the Superceding Indictment while attacking allegations that the United States does not make.

I. DEFENDANTS TOOK TRADITIONALLY RECOGNIZED PROPERTY RIGHTS FROM ONLINE TICKET VENDORS

In Count 1 and Counts 27 through 43, the Superceding Indictment charges defendants with conspiracy to commit wire fraud and substantive wire fraud, respectively. A sufficient charging document must allege these three elements of the substantive offense: (1) defendants’ knowing and willful participation in a scheme or artifice to defraud; (2) with the specific intent to defraud, and (3) the use of interstate wire communications in furtherance of the scheme. *United States v. Al Hedaithy*, 392 F.3d 580, 590 (3d Cir. 2006). Additionally, the object of the scheme or artifice to defraud must be a traditionally recognized property right. *Id.* (citing *United States v. Henry*, 29 F.3d 112, 115 (3d Cir. 1994)).

The object of defendants' fraud was to obtain — through lies and deceit, through shell corporations, and through unauthorized access to the victims' computer systems — approximately 1.5 million premium Event tickets and the rights associated with selling those tickets. Through Code-Based Restrictions and Contract-Based Restrictions, Online Ticket Vendors made clear again and again that they were unwilling to sell to Wiseguys. Online Ticket Vendors' restrictions failed, however, and defendants acquired precisely what Online Ticket Vendors would never have willingly sold them but for the fraudulent scheme.

Defendants complain that Wiseguys paid for all of the tickets and that there can therefore be no wire fraud. Def. Br. at 5-6 & 21 n.18. That Wiseguys paid for the tickets, however, does not end the inquiry. The Superceding Indictment alleges that defendants obtained both the tickets themselves and other traditionally recognized property rights: (1) the valuable right of Online Ticket Vendors to be the exclusive distributors of Event tickets on the primary ticket market (and the companion right of Venue Entities to choose their distributors); (2) the right to dictate the terms of sale for their product; and (3) the goodwill value associated with the perception that Online Ticket Vendors could distribute tickets fairly and in accordance with Venue Entities' wishes. Superceding Indictment, ¶ 2(c).

Defendants ask the Court to find that only tangible monetary interests are cognizable under the wire fraud statute. Def. Br. at 21. This is not the law. The mail and wire fraud statutes protect both tangible and non-tangible property interests. *See Cleveland v. United States*, 531 U.S. 12 (2000); *Carpenter v. United States*, 484 U.S. 19, 26, 27 (1987); *United States v. Al Hedaithy*, 392 F.3d 580, 603 (3d. Cir. 2004); *United States v. Schwartz*, 924 F.2d 410, 421 (2d Cir.1991); *see also United States v. Gray*, 405 F.3d 227, 234 (4th Cir. 2007) ("the mail and wire fraud statutes cover fraudulent schemes to deprive victims of their rights to control the

disposition of their assets").²

In *Carpenter*, an employee of the *Wall Street Journal* agreed with others to divulge the contents of a stock market column in advance of publication. 484 U.S. at 23. The employee, charged with wire fraud, argued that he committed no crime but had simply violated the *Wall Street Journal's* confidentiality rules. *Id.* at 25. The Supreme Court disagreed, holding that the mail and wire fraud statutes were not limited to deprivations of tangible property rights. “[T]he words ‘to defraud’ in the mail fraud statute have the common understanding of wronging one in his property rights by dishonest methods or schemes, and usually signify the deprivation of something of value by trick, deceit, chicane or overreaching.” *Id.* at 27 (internal quotations omitted). Specifically finding that monetary loss was not required, the Court held that the *Wall Street Journal* was deprived of a property right when defendant deprived it of the exclusive use of its information: “[I]t is sufficient that the Journal has been deprived of its right to exclusive use of the information, for exclusivity is an important aspect of confidential business information and most private property for that matter.” *Id.* at 26 (emphasis supplied).

Defendants' arguments that they violated only terms of service in buying tickets for commercial distribution sound like the ones the Supreme Court rejected in *Carpenter*. Defendants' protracted scheme to make themselves the distributors of 1.5 million tickets instead of Online Ticket Vendors took away exclusive sales rights that Online Ticket Vendors had bargained for, exclusivity being an “important aspect of ... most private property.” See *id.* at 26; Superceding Indictment, ¶ 2(c). This Court should reject defendants' arguments that all they

² The analysis under the mail and wire fraud statutes is the same. *Carpenter v. United States*, 484 U.S. 19, 25 n.6 (1987).

violated were internal rules.³

The Supreme Court revisited the question of “property” under the wire fraud statute in *Cleveland v. United States*, 531 U.S. 12 (2000). There, defendant pursued a fraudulent scheme to obtain licenses from a government entity. *Cleveland*, 531 U.S. at 16-17. The Supreme Court held that a governmental entity has no property rights in a license. *Id.* at 20-21. In reaching that conclusion, however, the Court explained that the result could be different in the private setting. For example, the Court recognized a franchisor’s right to select its franchisees as deriving from the franchisor’s ownership of a “trademark, brand name, business strategy or other product that the franchisor may trade or sell.” *Id.* at 24.

Here, Venue Entities had a right to choose an exclusive distributor, just as franchisors can choose franchisees under *Cleveland*. See *id.* Likewise, Online Ticket Vendors’ rights to be the exclusive distributors to certain Events and to choose how to distribute tickets are consistent with the suggestion in *Cleveland* that a business has a property interest in its business strategies. Defendants took away these rights from Venue Entities and Online Ticket Vendors when they decided to place themselves as middlemen between Venue Entities and the general public.

The Third Circuit’s controlling opinion in *United States v. Al Hedaithy*, which goes uncited by defendants, held that the mail and wire fraud statutes protect exclusivity rights and the right to control the sale of one’s property. 392 F.3d at 604. The scheme in *Al Hedaithy* involved defendants lying to the Educational Testing Service (“ETS”) about the true identity of test takers for the Test of English as a Foreign Language (“TOEFL”).

³ The Online Ticket Vendors have in fact sued to protect their exclusive distribution rights. <http://www.zdnet.com/news/ticketmaster-sues-ebays-stubhub-over-sales-tactics/151906> (visited Jul. 26, 2010) (Ticketmaster lawsuit alleging defendant StubHub, Inc. interfered with its Event Agreements, “which typically grant Ticketmaster exclusive rights to sell tickets for events to the general public”).

The *Al Hedaithy* indictment alleged a property right in the TOEFL test score, among other rights. The defendants argued that they paid for the tests and test scores and that they had therefore not deprived ETS of money or property. The defendants — like defendants in this case — also argued that the right to control one's property was not a property interest. *Id.* at 601. The Third Circuit disagreed. The court found that ETS had a property interest in its test scores. And the court expressly rejected the argument that the right to control one's property was not a recognized property interest. *Id.* at 603. With respect to ETS, the court found that there was a “deprivation of ETS’s right to exclusive use of its property.” *Id.* at 603.

In reaching its conclusion that the indictment alleged the taking of recognized property rights, including the right to control terms of sale, the Third Circuit expressly agreed with the Second Circuit’s analysis in *United States v. Schwartz*, 924 F.2d 410, 421 (2d Cir. 1991). *Id.* at 604 (“We agree with the Second Circuit’s analysis.”). In *Schwartz*, the defendants lied about their intentions and the identity of their customers in order to purchase night vision goggles from Litton Industries. Litton — which wanted to assure that its product were not sold illegally abroad — would not have sold to the defendants had it known the truth:

[T]he fact that Litton was paid for its night vision goggles does not mean that Litton received all it bargained for. In fact, it did not. Litton insisted its product not be exported from the country illegally and defendants' conduct deprived Litton of the right to define the terms for the sale of its property in that way, and cost it, as well, good will because equipment Litton, a government contractor, sold was exported illegally. The fact that Litton never suffered-and that defendants never intended it any pecuniary harm does not make the fraud statutes inapplicable. The record sufficiently demonstrates that Litton sold its products to appellants only because of their deceit and misrepresentations, which were offered as consideration for Litton to contract with them. Hence, appellants' convictions for wire fraud against Litton should be affirmed.

Al Hedaithy, 392 F.3d at 604 (quoting *Schwartz*, 924 F.2d at 421) (emphasis supplied).

In sum, the Third Circuit stated in *Al Hedaithy* that “[t]he only conclusion we draw from

the fact that ETS was paid in full is that ETS was not defrauded of any money. This fact, however, bears no relevance to whether ETS was otherwise defrauded of its property.” *Id.*

Defendants’ conduct here is no less a violation of the wire fraud statute. The Superceding Indictment contains specific allegations concerning Online Ticket Vendors’ right to define the terms of sale and the value of their goodwill. It further alleges that defendants lied in order obtain property — the tickets — much like the defendants in *Al Hedaithy* lied to obtain test scores and the defendants in *Schwartz* lied to obtain the night vision goggles.

Given the Third Circuit’s controlling precedent in *Al Hedaithy* and the Second Circuit’s persuasive analysis in *Schwartz*, this Court should find that payment is irrelevant here: the nature of the property rights taken was the same.

While they ignore *Al Hedaithy*, defendants focus on older and otherwise distinguishable cases, including *United States v. Alkaabi*, 223 F. Supp. 2d 583, 585 (D.N.J. 2002). Def. Br. at 23. In that TOEFL fraud case, the District Court (Orlofsky, J.) addressed charges against Alkaabi and another defendant, Tarik Alsugair. The only property right the United States alleged to have been taken was the integrity of ETS’ testing process. Judge Orlofsky found that property interest was not exclusive to ETS and therefore not cognizable under the mail and wire fraud provisions. *Alkaabi*, 223 F. Supp. at 590.

Alkaabi, however was not Judge Orlofsky’s final word on this issue. Responding to the decision in *Alkaabi*, the United States superceded parallel indictments in several TOEFL cases — including the case against Tarik Alsugair — and identified additional property interests that the defendants obtained during the scheme, including, among other rights, the value of ETS’ good will. *United States v. Alsugair*, 256 F. Supp.2d 306, 315 (D.N.J. 2003).

In *Alsugair*, which amazingly also goes uncited by defendants, Judge Orlofsky held that

the TOEFL fraud scheme's injury to a business' good will did fall within the scope of the mail fraud statute:

Alsugair ... argues that he cannot be charged with mail fraud based on ETS's loss of goodwill because goodwill cannot be transferred separately from the business with which it is associated. This, however, requires a holistic conceptualization of goodwill, and the mail-fraud statute requires no such thing. A business may be "deprived" of its goodwill whether the goodwill is transferred in its entirety, or made less valuable in part. To conclude otherwise would permit a defendant to cripple a business for an extended period of time without fear of retribution, unless and until the business collapsed and a "total" loss resulted.

Alsugair, 256 F. Supp.2d at 315 & n. 11 (internal citations omitted).

Defendants also cite *United States v. Henry*, decided 10 years before *Al Hedaithy*, where defendant was charged with fraud for rigging the bid process for a government contract by disclosing confidential bids. 29 F.3d 112, 113 (3d Cir. 1994); Def. Br. at 21. The indictment in *Henry* alleged that the fraud's victims were banks who lost the chance to bid fairly on the contracts. The Third Circuit found that this right was too attenuated to constitute a property right. Defendants' reliance on *Henry* is misplaced. The United States does not allege that Wiseguys defrauded other ticket brokers by denying them the chance to buy tickets. The Superceding Indictment alleges Wiseguys defrauded Online Ticket Vendors and Venue Entities by depriving them of exclusive and valuable property rights, facts consistent with *Schwartz* and *Al Hedaithy*, not *Henry*.

United States v. Bruchhausen, 977 F.2d 464 (9th Cir. 1992), offers no safe harbor to defendants. In *Bruchhausen*, a defendant convicted of wire fraud lied to American manufacturers about the ultimate destination of certain technologies that the defendant wanted to purchase. The victims would not have sold to the defendant had they known that he was going to export their products to the Soviet Bloc. 977 F.2d at 466.

In an usual decision, the Ninth Circuit provided no true majority opinion. Two judges on the panel wrote conflicting opinions, while the third judge joined both. Judge Canby, whom defendants cite, Def. Br. at 22-23, wrote an opinion rejecting the Second Circuit's opinion in *Schwartz*, where he stated that "the interest of the manufacturers in seeing that the products they sold were not shipped to the Soviet Bloc in violation of federal law is not 'property' of the kind that Congress intended to reach in the wire fraud statute." *Bruchhausen*, 977 F.2d at 466 (Canby, J., joined by Kozinski, J.). Judge Fernandez, however, agreed with the analysis in *Schwartz*:

In my opinion, at the very least ownership of a tangible object, whether it is a pen, a desk or a piece of equipment, includes the right to retain that object and to refuse to transfer it to others. The right persists even if others are willing to pay fair market value for the object. ... The strictures an owner puts on his willingness to sell an item are not mere ephemera. When a prospective buyer lies in order to evade those strictures, a fraud has been committed upon the owner of the item just as surely as if the buyer had issued a rubber check.

Id. at 469 (Fernandez, J., concurring, joined by Kozinski, J.). Judge Fernandez voted to reverse the conviction only because the United States had not pled the purchase of property through deceit, which for him would have been sufficient. *Id.* at 470. The Superceding Indictment does plead that property interest. ¶ 2(c).

Subsequent panels of the Ninth Circuit have agreed with Judges Fernandez and Kozinski. *United States v. Harper*, 32 F.3d 1387 (9th Cir. 1994) ("The strictures an owner puts on his willingness to sell an item are not mere ephemera. When a prospective buyer lies in order to evade those strictures, a fraud has been committed upon the owner of the item...."); *United States v. DiFronzo*, 26 F.3d 133 (9th Cir. 1994) (non-precedential) ("even though defendants may have been willing to pay fair market value ..., their actions violate the mail and wire fraud statutes because they intended to obtain the [victim's] property by misrepresenting the identity of the investors.").

Defendants now suggest that the rights to select distributors, to control terms of sale, and to keep business good will are not worthy of the wire fraud statute's protection. But *ante lite motam*, they had a very different position. Defendants' establishment of REM — a company that marketed itself as better able to distribute tickets to the public than Online Ticket Vendors — shows their true goal. Superceding Indictment, ¶¶ 41-42. Having damaged Online Ticket Vendors' goodwill — which relied in part on the perception that Online Ticket Vendors could fairly distribute tickets, *Id.*, ¶ 2(c) — defendants offered themselves as the solution to a problem that they had created. The Superceding Indictment thus alleges not only a conspiracy to deprive Online Ticket Vendors of their good will and exclusivity, but a conspiracy to step in and take the very distribution right that defendants now claim is not cognizable. *See Alsugair*, 256 F. Supp.2d at 316 ("A business may be deprived' of its goodwill whether the goodwill is transferred in its entirety, or made less valuable in part.").⁴

The Court should follow the Third Circuit's controlling precedent in *Al Hedaithy*; the Second Circuit in *Schwartz*; and reject the "majority" opinion in *Bruchhausen*. Because the Superceding Indictment alleges the taking of recognized property interests, this Court should deny the motion to dismiss Counts 27 through 43.

⁴ In this regard, *amicus'* discussion of the economics and public policy of Event ticketing is misplaced. Confronted with purportedly anti-competitive behavior, defendants did not hire top-notch antitrust counsel. They wrongfully helped themselves to the product. *United States v. Weinstein*, 762 F.2d 1522, 1533 (11th Cir. 1985) ("The merits of [the victims'] claims of right to sell drugs domestically at a uniform price is immaterial to the issue of fraud. If defendants doubted the legality of that practice their recourse would have been through antitrust action, not through a scheme of misrepresentations communicated through U.S. mails and wires.")

II. DEFENDANTS CIRCUMVENTED CODE-BASED AND CONTRACT-BASED RESTRICTIONS ON ACCESS IN VIOLATION OF SECTION 1030

The Superceding Indictment alleges that Online Ticket Vendors restricted access to their websites through security measures, including IP Blocks, Buypage Encryption, CAPTCHA, Proof of Work, cease and desist demands, terms of service, and litigation. Defendants ignore all of these allegations except for terms of service. Moreover, defendants try to rewrite the Superceding Indictment, attacking “the *government’s theory* that alleged breaches of online terms of use constitute unauthorized access.” Def. Br. at 8 (emphasis supplied). This, however, is not the government’s theory. Defendants’ entire argument regarding “unauthorized access” is based on the false premise that the Superceding Indictment alleges unauthorized access solely in violation of terms of service. *Id.* at 7-17. In ten pages of argument, defendants never discuss IP Blocks, Proof of Work, CAPTCHA or Buypage Encryption. Nor do defendants discuss the cease and desist letters they received. *Amici* similarly fail to acknowledge these measures anywhere in their briefs. Accordingly, both are briefing an issue — whether terms of use or contract-based restrictions alone can underlie Section 1030 criminal liability — that is not before this Court.⁵

The Superceding Indictment sets forth numerous Code-Based Restrictions on access (as well as Contract-Based Restrictions). The first line of defense against automated computers was Buypage Encryption. Buypage Encryption completely blocked direct access to Buypages. Conspiring to defeat such encryption is akin to drilling through the side of a bank vault, and the Superceding Indictment more than sufficiently alleges that defendants conspired to do just that. Superceding Indictment, ¶ 9(c). Next, the Online Ticket Vendors deployed various CAPTCHA

⁵ Defendants appear so intent on ignoring the charges in the Superceding Indictment that they characterize the government’s case based on introductory language to search warrants from “the very inception of the case,” rather than the Superceding Indictment itself. Def. Br. at 4.

protections, a computer code used by e-Commerce sites to block access to automated computers. Whether viewed as a password for human users or a bar on automated programs, CAPTCHA is computer code designed to keep out automated programs. Indeed, the only court to consider whether CAPTCHA was designed to prevent access had no difficulty in finding that it does: “[CAPTCHA is a] technological measure that regulates access.” *Ticketmaster LLC v. RMG Technologies*, 507 F. Supp. 2d 1096, 1112 (C.D. Cal. 2007). The next Code-Based Restriction on access was the IP Blocks. Defendants ignore entirely the Superceding Indictment’s allegations that Online Ticket Vendors blocked defendants’ unwelcome access thousands of times. *Amici* contradict this part of the Superceding Indictment and instead represent to the Court, without citation, that “OTVs . . . implement no checks on who may use the service.” Am. Br. at 18. To the contrary, these thousands of IP Blocks were unmistakable restrictions on access and clear notice to defendants that they were not authorized to access Online Ticket Vendors’ computers. Finally, the Superceding Indictment alleges that the defendants circumvented Proof of Work protections, computer code built into Ticketmaster’s website to deter access to automated programs. There are thus Code-Based Restrictions on access alleged in the Superceding Indictment that unambiguously define defendants’ conduct as unauthorized access.

Defendants cite no case holding that repeated access violating Code-Based Restrictions is somehow authorized. The Government is aware of no such holding. Nor are there cases holding otherwise, since it is a self evident proposition that violating Code-Based Restrictions is unauthorized. Recently, in examining access to Facebook’s computers “without permission” under a California criminal statute similar to Section 1030, the Court in *Facebook v. Power Ventures, Inc.*, No. C. 08-05780 JW (N.D. Cal. Jul. 20, 2010) (“Facebook”), recently recognized: a distinction ... between access that violates a term of use and access that

circumvents technical or code-based barriers that a computer network or website administrator erects to restrict the user's privileges within the system, or to bar the user from the system altogether. Limiting criminal liability to circumstances in which a user gains access to a computer, computer network, or website to which access was restricted through technological means eliminates any constitutional notice concerns, since a person applying the technical skill necessary to overcome such a barrier will almost always understand that any access gained through such action is unauthorized.

Facebook at 18 (emphasis added) (Attached hereto as Exhibit 1) (citing Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1650-51 (2003)).

Defendants and amicus may suggest that Online Ticket Vendors' Code-Based Restrictions were inadequate, or that these security protections somehow lose their force because they were simply enforcing contractual limits on access. As an initial matter, these arguments challenge the United States' factual allegations and are premature. *Panarella*, 277 F.3d at 681 ("For purposes of determining the sufficiency of [a charging document], we assume the truth of the following facts alleged....").

Moreover, it cannot be that only security measures worthy of the National Security Agency's use deserve protection under Section 1030. An argument that a victim could have prevented access by installing a stronger security mechanism is akin to a "thief arguing that 'I would not have been able to steal your television if you had installed deadbolts instead of that silly lock I could open with a credit card.'" *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 936 (9th Cir. 2004) (rejecting defendants' argument that victim should have installed a computer security patch to prevent automated access to the victims' computer networks).

Finally, to suggest that the existence of terms of service render Code-Based Restrictions on access meaningless would convert all security measures into mere terms of use. Open season

would ensue — with no criminal consequence — on any website with terms of service regarding access to the site. “The owner’s underlying purpose or motivation for implementing technical barriers, whether to enforce terms of use or otherwise, is not a relevant consideration when determining the appropriate scope of liability for accessing a computer or network without authorization.” *Facebook* at 19-20.

The Superceding Indictment alleges that defendants knew that Online Ticket Vendors sought to block their access through computer code. To defeat these security measures, defendants employed computer programmers. These computer programmers talked about “backdoors,” “tricks,” “hacks,” and beating encryption. Superceding Indictment, ¶¶ 9(e) & 43(d). The computer programmers wrote code to beat the victims’ code, including code to circumvent CAPTCHA and Audio CAPTCHA using the CAPTCHA Bots;⁶ code to employ a nationwide network of computers, *id.*, ¶ 10, and code to avoid IP Blocks and continue to access the websites. Defendants wrote and commissioned this code because Online Ticket Vendors denied automated programs access to their computer networks.

Had Online Ticket Vendors simply blocked access via “terms of use” or “contract-based” restrictions, there would have been no need for Bulgarian computer programmers, OCR software, and massive networks of computers. For this reason, defendants’ motion to dismiss completely misses the mark and should be denied.

Questions of “Access” Arise Only in Cases Involving Significantly Different Restrictions than Those in the Present Case

As discussed above, the Government knows of no case in which a court has held that violating Code-Based Restrictions on access (with or without accompanying Contract-Based

⁶ The Superceding Indictment’s term for defendants’ automated ticket purchasing system.

Restrictions) was insufficient to establish unauthorized access under Section 1030. The Court should deny defendants' motion to dismiss on this basis alone.

Additionally, two Courts of Appeals considering unauthorized access in the context of Section 1030 have found criminal violations even absent the combination of Code- and Contract-Based Restrictions alleged in the Superceding Indictment. *See, e.g., United States v. John*, 597 F.3d 263, 271 (5th Cir. 2010); *United States v. Salum*, 257 Fed. Appx. 225, 230 (11th Cir. 2007) (non-precedential). In *John* and *Salum*, the defendants were employees charged solely with violating contractual restrictions on certain uses of computers to which they otherwise had authorized access. In *John*, the defendant was a bank employee who accessed account records to take customer information in furtherance of a fraud scheme. *John*, 597 F.3d at 269. In *Salum*, the defendant was a police officer who had authority to access criminal histories but used that access improperly by giving data to a private investigator. *Salum*, 257 Fed. Appx. at 230. In post-conviction appeals challenging the sufficiency of the evidence introduced at trial, The Fifth and Eleventh Circuits, respectively, found that each defendant's access was unauthorized under Section 1030. *John*, 597 F.3d at 271; *Salum*, 257 Fed Appx. at 230.

In the civil context, the answer has been no different. Cases alleging only terms of use violations (*i.e.*, alleging none of the circumvention of code-based restrictions present in the Superceding Indictment) led to findings of unauthorized access in violation of Section 1030. *See, e.g., eBay, Inc. v. Digital Point Solutions, Inc.* 608 F. Supp. 2d 1156, 1164 (N.D. Cal. 2009) (motion to dismiss Section 1030 claim based on "allegations with respect to access and use beyond those set forth in a user agreement"); *Register, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238, 251 (S.D.N.Y. 2000), *aff'd in part and reversed in part on other grounds*, 356 F.3d 393 (2d Cir.2004); *America Online Inc. v. LCGM, Inc.* 46 F. Supp. 2d 444, 450 (E.D. Va 1998)

(“Defendant’s actions violated AOL’s terms of service, and as such was [sic] unauthorized.”); *see also EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 62 (1st Cir. 2003) (finding violation of agreement constituted unauthorized access).

The combination of Code-Based and Contract-Based Restrictions on access in the Superceding Indictment are far more robust than the terms of service in the cases described above that established Section 1030 violations. There can thus be no question that the allegations in the Superceding Indictment sufficiently set forth a violation of Section 1030. Arguments to the contrary are fact driven and inappropriate in a pretrial motion to dismiss. “It is now well-established that, at this stage of a criminal action, the court may not look[] beyond the face of the indictment and rul[e] on the merits of the charges against [a defendant].” *United States v. Salman*, 378 F.3d 1266, 1267 (11th Cir.2004) (internal quotations omitted).

Defendants correctly cite a number of the cases above but ask this Court to disregard them “civil decisions.” Def. Br. at 15. There is no basis for such a request. The Supreme Court has stated that where statutory sections contains both civil and criminal remedies, civil opinions deserve the same weight as criminal opinions. *See Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004); *see also LVRC Holdings v. Brekka*, 581 F.3d 1127, 1134 (9th Cir. 2009) (interpretation of Section 1030 is the same for both criminal and civil matters).

Defendants also cite a number of cases for the proposition that contractual limitations on users’ *subsequent use* of data (*i.e.*, after they obtained lawful access) were insufficient to establish unauthorized access to a computer holding that data. Def. Br. at 13-14 (citing *Brekka*, 581 F.3d at 1135; *United States v. Nosal*, 2010 WL 934257, *6 (N.D. Cal. Jan. 6, 2010); *Brett Senior & Assocs. v. Fitzgerald*, 2007 WL 2043377 (E.D.P.A. July 13, 2007); *Int’l Ass’n of*

Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479 (D. Md. 2005)). In each of these cases, employers had authorized the defendants to access their computers, but they had not permitted access for the defendants' intended purpose. For example, in *Brekka*, the defendant employee took a job with a competing company. Prior to leaving his employer, he used his computer to access some documents and e-mail those documents to his personal e-mail account. 581 F.3d at 1129-30. The court rejected Section 1030 liability because Brekka's *access* was authorized, it was just that his employer attempted to limit the *purpose* (or "intended use") for which access was granted. *Id.* at 1133. *Fitzgerald*, *Nosal*, and *Werner-Masuda* similarly rejected Section 1030 liability based on those defendants' use of information obtained through otherwise permitted access. *Fitzgerald*, 2007 WL 2043377 at *4; *Nosal*, 2010 WL 934257 at *6; *Werner-Masuda*, 390 F. Supp.2d at 498.

These cases do not support dismissal for three reasons. First, the cases relate solely to contract-based restrictions, and this case involves a combination of Code-Based Restrictions and Contract-Based Restrictions. Second, Online Ticket Vendors restricted access through the Code- and Contract-Based restrictions no matter the user's purpose in accessing the computer. That is, the Code- and Contract-Based Restrictions blocked automated programs' access to Buypages no matter whether the automated program was seeking access to take an inventory of tickets, to purchase tickets, or otherwise to collect data. Finally, as discussed above, circuits other than the Ninth Circuit have found Section 1030 unauthorized access based solely on restrictions on a defendant's intended use. See, e.g., *John*, 597 F.3d at 271; *Salum*, 257 Fed. Appx. at 230; see also *Int'l Airport Centers v. Citrin*, 440 F.3d 418 (7th Cir. 2006) (authorization ends when an employee chooses to act against the interests of the business).

III. THE CHARGES IN THE SUPERCEDING INDICTMENT ARE NOT VAGUE, AND THE RULE OF LENITY IS INAPPLICABLE

Relying primarily on the decision in *United States v. Drew*, 259 F.R.D. 449 (N.D. Cal. 2009), defendants argue that the Superceding Indictment must be dismissed because Section 1030 is void for vagueness as applied to the facts of this case. Def. Br. at 10-13.

The Third Circuit recently summarized its law on vagueness challenges this way:

A statute is void on vagueness grounds if it: (1) fails to provide people of ordinary intelligence a reasonable opportunity to understand what conduct it prohibits; or (2) authorizes or even encourages arbitrary and discriminatory enforcement.... The inquiry is undertaken on a case-by-case basis, and a reviewing court must determine whether the statute is vague as-applied to the affected party.... In the criminal context, the Supreme Court has held that since vagueness attacks are based on lack of notice, they may be overcome in any specific case where reasonable persons would know their conduct puts them at risk of punishment under the statute.... Therefore, for a criminal statute to be constitutional, criminal statutes need only give fair warning that certain conduct is prohibited.... In addition, the Supreme Court has held that scienter requirements in criminal statutes “alleviate vagueness concerns,” because a *mens rea* element makes it less likely that a defendant will be convicted for an action that he or she committed by mistake.

United States v. Fullmer, 584 F.3d 132, 152 (3d Cir. 2009) (citations and quotations omitted).

As a threshold matter, however, the Supreme Court has held that “[i]t is well established that vagueness challenges to statutes which do not involve First Amendment freedoms must be examined in the light of the facts of the case at hand.” *United States v. Mazurie*, 419 U.S. 544, 550 (1975). “‘As applied’ review requires a court to review the specific facts in the case to determine if a reasonable person in [d]efendants’ position would have been on notice that their conduct was at risk. These types of factual determinations are not appropriately determined by a court in a pretrial motion.” *United States v. Caputo*, 288 F. Supp.2d 912 (N.D. Ill. 2003); *see also United States v. Reed*, 114 F.3d 1067 (10th Cir. 1997) (reversing as premature dismissal

pretrial for vagueness as applied: “it is necessary that the evidence in the case be presented before the task of statutory construction can be properly completed”); *United States v. Coronado*, 461 F. Supp.2d 1209 (S.D. Cal. 2006) (“any ruling on the as applied challenges to contested proffered facts is speculative” at pretrial motions stage). Given this standard, the Court should decline defendants’ premature invitation to engage in an as- applied analysis of Section 1030.

Given the facts alleged in the Superceding Indictment and the standard in *Fullmer*, it is in any event impossible to conclude that defendants lacked notice that their conduct was illegal. Beyond the technical barriers that defendants defeated, and beyond the unambiguous notice to them that their access was unauthorized, defendants acted like people who knew their access was not permitted. Defendants lied about who they were. Superceding Indictment, ¶¶ 36(b), 46(b) & 46(f). They lied about their business model. *Id.*, ¶¶ 38 & 46(d). They lied when they impersonated thousands of individual ticket buyers. *Id.*, ¶ 1(a). They lied when the established thousands of false e-mail addresses and domain names. *Id.*, ¶¶ 46(b) & 49. They avoided getting caught by planning and deploying “stealth measures.” *Id.*, ¶¶ 36 & 47(e). Defendants tried to hide their actions because they knew they were breaking the law. “Defendants cannot,” therefore, “argue that the statute was vague.” See *Fullmer*, 584 F.3d at 153.

Defendants’ reliance on *Drew* is misplaced. First, the allegations in *Drew* were only that Lori Drew exceeded authorized access because she violated a website’s terms of service:

[T]he only basis for finding that Drew intentionally accessed MySpace’s computer/servers without authorization and/or in excess of authorization was her . . . violations of the [terms of service] by deliberately creating [a] false [] profile, posting a photograph of a juvenile without his permission and pretending to be a sixteen year old O’Fallon resident for the purpose of communicating with Megan. Therefore, if conscious violations of the MySpace terms of service were not sufficient to satisfy the first element of the [Section 1030] misdemeanor violation

as per [Sections 1030(a)(2)(C) and (b)(2)(A)], Drew's Rule 29(c) motion would have to be granted on that basis alone.

Unlike this case, *Drew* involved no allegations of code-based restrictions on access. This point cannot be overstated because the underpinning of *Drew* is that it was only a terms of use case.

Second, although *Drew* found that there were significant notice issues concerning MySpace's restrictions on access (i.e., Ms. Drew may not have read or understood that her access was in violation of terms of service), it understood that:

While issues might be raised in particular cases as to the sufficiency of the notice and/or sufficiency of the user's assent to the terms, and while public policy considerations might in turn limit enforcement of particular restrictions, the vast majority of the courts (that have considered the issue) have held that a website's terms of service/use can define what is (and/or is not) authorized access vis-a-vis that website.

Id. at 461 (internal citations omitted) (emphasis supplied).

In this prosecution, there can be no suggestion that defendants were unaware of Online Ticket Vendors' restrictions, whether Contract- or Code-Based. Indeed, defendants received cease and desist letters and discussed methods to ignore and evade such demands. Superceding Indictment, ¶¶ 38 & 46(f). To the extent that defendants challenge the allegations of notice, a trial is the appropriate venue for determining that issue.

Third, *Drew* addressed a defendant who accessed a computer system for a non-commercial, personal matter. Here, defendants accessed Online Ticket Vendors' sites solely for commercial gain. Cf. S. Rep. 104-357, 104th Congress, 2nd Session, 1996 WL 492169 at 8 (1996) (Section 1030 targets for felony treatment access offenses committed for purpose of commercial advantage or private financial gain).

Drew thus supports a Section 1030 prosecution where, as here, there are Code-Based

Restrictions, a strong commercial motive for the unauthorized access, and no actual notice issues regarding defendants' access. As the court stated in *Facebook*, “[t]here can be no ambiguity or mistake as to whether access has been authorized when one encounters a technical block, and thus there is no potential failure of notice to the computer user as to what conduct may be subject to criminal liability, as when a violation of terms of use is the sole basis for liability.” *Facebook* at 19-20 (questions of material fact regarding whether defendants circumvented technical barriers to access precluded summary judgment). Given the multitude of code-based restriction, even under *Drew* there is thus no place for the rule of lenity in this case.

This Court should leave defendants' parade of hypotheticals for another day. *See Fullmer*, 584 F.3d at 153 (rejecting “speculation as to the hypothetical ways that [a statute] could be unconstitutionally vague”). Defendants were not children using Google in violation of its terms of service. Defendants wrote and directed computer programs to defeat technical barriers meant to keep them out of the victims’ computers. The Superceding Indictment is susceptible to no interpretation other than that defendants’ access was unauthorized, that they knew it, and that they did not take “NO!” for an answer. The Section 1030 Counts properly allege unauthorized access, and the Court should deny any motion to dismiss suggesting otherwise.

IV. COUNTS 11 THROUGH 20 OF THE SUPERCEDING INDICTMENT DISTINCTLY ALLEGE UNAUTHORIZED ACCESS AND FRAUD

Defendants assert incorrectly that Counts 11 through 20 of the Superceding Indictment “conflate the alleged ‘fraud’ with the alleged ‘unauthorized access.’” Def. Br. at 18. To the contrary, the Superceding Indictment charges defendants with distinct elements. First, defendants gained unauthorized access to the victims’ computers by defeating IP Blocking,

CAPTCHA, Proof of Work, and other Code-Based Restrictions. The Court need not analyze defendants' motive for access to determine that the access was unauthorized. Defendants' intended fraud, by contrast, was the fraud scheme to deprive Online Ticket Vendors and Venue Entities of their bargained-for rights to select and be, respectively, the exclusive distributors of Event tickets, their right to dictate the terms of sale of Event tickets, and their good will.

The Superceding Indictment does not allege that the fraud scheme was the use of automation to gain access. Instead, once in the victims' systems, defendants defrauded Online Ticket Vendors by deceiving them into believing they were selling to individual ticket buyers. The false e-mail addresses used to purchase Event tickets, the telephone calls in which defendants impersonated others, and the false statements defendants made to establish their nationwide computer infrastructure, among other deceptions, all served to obtain Event tickets against the Online Ticket Vendors' wishes, not to bypass CAPTCHA and other Code-Based Restrictions to gain access to the ticketing systems.

The charges in Counts 11 through 20 are therefore entirely consistent with the suggestion in *Fitzgerald*, 2007 WL 2043377 at *4, that the Court not consider a defendant's motives for accessing computers in deciding whether their access was authorized. In fact, that computers are the locus of both the access and the fraud in this case should not be surprising, considering Congress' intention that the use of the computer in a Section 1030 prosecution be "integral to the perpetration of a fraud." See *id.* (citing S. Rep. 99-432 at 8-9 (1986)).

Because the Superceding Indictment alleges the "access" and "fraud" elements of Section 1030(a)(4) distinctly, the Court should deny defendants' motion to dismiss Counts 11 through 20.

V. DEFENDANTS OBTAINED “INFORMATION” UNDER SECTION 1030(a)(2)(C)

Defendants argue incorrectly that they obtained no “information” within the meaning of Section 1030. Def. Br. at 17-18. Congress placed no limit on the kind of information that could be obtained in violation of Section 1030(a)(2)(C), and the legislative history of subsection (a)(2)(C), discussed below, makes clear that either viewing information or obtaining it would meet the “obtains information” element of Section 1030. The Superceding Indictment alleges that defendants both viewed and obtained a wide variety of information.

Subsections (a)(1), (a)(2)(A), and (a)(2)(B) of Section 1030 expressly protect classified national security information, financial records, and information from any federal department or agency, respectively. Subsection (a)(2)(C), however, is silent on what kind of information must be obtained to establish an element of the crime and therefore applies to the taking of any information. Had Congress wished to limit the kind of information protected from unauthorized access, it certainly knew how to do so. *Hartford Underwriters Ins. Co. v. Union Planters Bank, N.A.*, 530 U.S. 1 (2000) (“we begin with the understanding that Congress “says in a statute what it means and means in a statute what it says there”).

Defendants assert that “it should go without saying that tickets are not information,” Def. Br. at 17, while ignoring nearly every piece of information defendants obtained regarding those tickets. The CAPTCHA Bots automatically gathered for defendants’ purchasing process the exact section, rows, and seat numbers of dozens of available premium seats for each Event. The defendants thus clearly obtained information.

Congress also made clear that to “obtain information” under Section 1030, one must do no more than read or view data or information from an Internet-connected computer. In a 1986

Senate Judiciary Committee report, legislators sought to “make clear that ‘obtaining information’ in this context includes mere observation of data. Actual asportation need not be proved in order to establish a violation of this subsection.” S. Rep. No. 99-432 at 6-7 (1986), reprinted at 1986 U.S.C.C.A.N. 2479, 2484. In 1996, Congress amended Section 1030 again and the Senate Judiciary Committee again reported that “the term ‘obtaining information’ includes merely reading it.” S. Rep. 104-357, 104th Cong., 2nd Sess. 1996, 1996 WL 492169. Defendants thus obtained information when they scoured Online Ticket Vendors’ websites for available seats.

See Healthcare Advocates v. Harding, Earley, Follmer & Frailey, 497 F. Supp. 2d 627 (E.D.P.A. 2007) (viewing webpage screenshots over the Internet constituted obtaining information).

At every opportunity, defendants attempt to collapse the “obtains information” element of Section 1030 with the separate element of unauthorized access. Def. Br. at 17. No matter how appealing (or irrelevant) their argument on whether contractual terms can define authorized access, an alarming hypothetical imposing criminal liability on any Internet search has no place in a discussion of what it means to “obtain information” under Section 1030(a)(2)(C). Even *Drew*, defendants’ guiding light on matters of authorized access, makes clear that “the latter two elements of the section 1030(a)(2)(C) crime,” that is, obtaining information and accessing an interstate computer, “will always be met when an individual using a computer contacts or communicates with an Internet website.” 259 F.R.D. at 457 (emphasis supplied).

Finally, defendants obtained information under Section 1030 even if subsection (a)(2)(C) somehow silently requires that information obtained not be otherwise publicly available. The information defendants obtained and exploited for their financial gain — the specific location and availability of entire blocks of premium Event tickets — was not available to any user

visiting Online Ticket Vendors' websites. Authorized users could only see a limited number of available tickets to a single event, not the virtual seat map that the CAPTCHA Bots assembled for defendants.

Accordingly, defendants did obtain information that was confidential in the aggregate, where the public could only view some of it. Under similar circumstances, America Online has successfully sued bulk e-mailers under Section 1030 for obtaining "information" when the bulk e-mailers signed up for AOL accounts to obtain and sell the e-mail addresses of fellow AOL members. Although AOL's e-mail addresses were available publicly to its members, the Court ruled that "the addresses of AOL members are 'information' within the meaning of the Act because they are proprietary in nature." *America Online v. LCGM, Inc.*, 46 F. Supp. 2d 444 (E.D. Va 1998); *America Online v. National Health Care Discount, Inc.*, 121 F. Supp. 2d. 1255 (N.D. Iowa 2000).

Because Counts 2 through 10 of the Superceding Indictment allege that defendants obtained "information" within the meaning of Section 1030(a)(2)(C), the Court should deny defendants' motion to dismiss regarding those counts.

VI. DEFENDANTS DAMAGED ONLINE TICKET VENDORS' COMPUTERS BY IMPAIRING THE AVAILABILITY OF DATA WITHOUT AUTHORIZATION

Counts 21 through 26 of the Superceding Indictment properly allege that defendants damaged Online Ticket Vendors' computers without authorization within the meaning of 18 U.S.C. § 1030(a)(5). In the minutes after Event tickets went on sale, the competition for tickets and ticketing information was a zero-sum game. When the CAPTCHA Bots seized hundreds of the best available tickets and permitted Wiseguys to determine which of those it would purchase,

no other user could access that information. Superceding Indictment, ¶ 25 (“It was further part of the conspiracy that, when the CAPTCHA Bots seized the best available seats from the Online Ticket Vendors’ networks, those same tickets were unavailable for purchase or consideration by any authorized user of the Online Ticket Vendors’ websites until a Wiseguys employee released those seats.”).

Section 1030 broadly defines “damage” to include “any impairment to the integrity or availability of data, a program, a system, or information.” 18 U.S.C. § 1030(e)(8) (emphasis added). As detailed in the Superceding Indictment, defendants’ unauthorized access to Online Ticket Vendors’ websites allowed them to monopolize Buypages for hundreds of tickets at a time. Because Online Ticket Vendors could not show available seats to more than one person at a time, they could not send Buypages for seats that defendants had seized to legitimate customers. Thus, defendants’ unauthorized access had the result of “impairing” the “availability” of “data” and “information” — namely, the Buypages. Quite simply, while defendants were on Online Ticket Vendors’ systems without authorization, authorized users could not access tickets that Wiseguys employees were considering and purchasing.

In *United States v. Carlson*, the defendant was an avid baseball fan and savvy Internet user. 209 Fed. Appx. 181, 2006 WL 3770611 (3d Cir. 2006) (non-precedential). The defendant was convicted of causing damage under Section 1030(a)(5) when he caused thousands of e-mails to flood his targets’ e-mail accounts. *Carlson*, 109 Fed. Appx. at 185. The Third Circuit affirmed his conviction, finding that the defendant intended to damage his victims by clogging their computers, causing delays, and at times causing valuable business-related e-mails to be permanently lost. Here, as in *Carlson*, defendants flooded Online Ticket Vendors’ systems with

Buypage requests, clogging their computers and preventing Online Ticket Vendors from granting access to Buypages to their authorized users. *See also United States v. Schuster*, 467 F.3d 614, 616 (7th Cir. 2006) (defendant's access damaged victim's network within the meaning of Section 1030(a)(5) by impairing the availability of the network to legitimate customers); *National Health Care*, 121 F. Supp. at 1274 & n.18 (“when a large volume of unsolicited business e-mail causes slowdowns or diminishes the capacity of AOL to serve its customers, an ‘impairment’ has occurred to the availability of AOL’s ‘system.’”); *Ford v. Torres*, 2009 WL 537563, *9 (E.D. Va. Mar. 3, 2009) (“Defendants ‘damage[d]’ the [plaintiff] by ‘impair[ing] … the availability of data’ to a party entitled to the data”); *Cf. Moulton v. VC3*, 2000 WL 33310901, *6 (N.D. Ga. Nov. 7, 2000) (damage element of Section 1030(a)(5) not satisfied where defendant’s automated scanning program did not impair the availability of information on the victim’s network).

Defendants indirectly suggest, Def. Br. at 20, that when any user is at a Buypage selecting tickets, that impairs the availability and integrity of ticket data. The difference between “any user” and defendants, however, is that other users were authorized to view Buypages and impair the availability of data, whereas when defendants did so by using automated means, they were not.

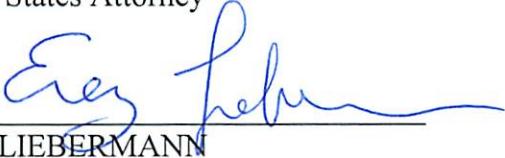
Because the Superceding Indictment alleges that defendants damaged Online Ticket Vendors networks by impairing the availability of data to authorized users, the Court should deny defendants’ motion to dismiss Counts 21 through 26.

CONCLUSION

For all of the reasons above, the United States requests that the Court deny defendants' motion to dismiss the Superceding Indictment.

Respectfully submitted,

PAUL J. FISHMAN
United States Attorney

By: 
EREZ LIEBERMANN
SETH B. KOSTO
Assistant United States Attorneys

JOSH GOLDFOOT
Trial Attorney
United States Department of Justice

August 2, 2010
Newark, New Jersey

CERTIFICATE OF SERVICE

I hereby certify that on the 2nd day of August 2010, a true and correct copy of the United States' Opposition to Defendants' Motion to Dismiss the Superceding Indictment was served by electronic filing upon the individuals below.

/s/Seth B. Kosto
SETH B. KOSTO
EREZ LIEBERMANN
Assistant United States Attorneys

Mark A. Rush, Esq.
Andrew R. Stanton
K&L Gates LLP
K&L Gates Center
210 Sixth Avenue
Pittsburgh, PA 15222-2613

David S. Kwon, Esq.
K&L Gates LLP
One Newark Center, 10th Floor
Newark, NJ 07102

Richard Coughlin, Esq.
John H. Yauch, Esq.
Office of the Federal Public Defender for the
District of New Jersey
1002 Broad Street
Newark, NJ 07102

John P. McDonald
McDonald & Rogers LLC
181 West High Street
Somerville, NJ 08876
One Newark Center, Tenth Floor
Newark, New Jersey 07102
Telephone: 973.848.4000